UNCLASSIFIED

AD-A284 284

AR-008-866

DEPARTMENT OF DEFENCE

# DSTO

## Communications Division

DTIC ELECTE SEP 09 1994 S B D

ELECTRONICS RESEARCH LABORATORY

REPORT
ERL-0825-RE

# AN INTRODUCTION TO INTELLIGENT NETWORKS

by

Wolf Getto

94-29581

DTIC QUALITY INSPECTED 3

APPROVED FOR PUBLIC RELEASE

UNCLASSIFIED

AR-008-866

DSTO
AUSTRALIA

ELECTRONICS RESEARCH LABORATORY

# Communications Division

REPORT
ERL-0825-RE

## AN INTRODUCTION TO INTELLIGENT NETWORKS

by

Wolf Getto

SUMMARY

intelligent networking is a new and developing technology that is already having significant impact on telecommunications architectures. This paper offers a summary of this technology, concluding with a brief discussion of how it is likely to affect the military communications of the ADF.



Issue 1
Feb-94



APPROVED FOR PUBLIC RELEASE

POSTAL ADDRESS: Head, SSN Group, Communications Division, ERL,
PO Box 1500, Salisbury, South Australia, 5108

# CONTENTS

Page No.



## FIGURES



## TABLES

# APPENDICES

# ABBREVIATIONS

## 1 General

| | |
|---|---|
| ADF | Australian Defence Force |
| B-ISDN | Broadband Integrated Services Digital Network |
| BCSM | Basic Call State Model |
| $C^3I$ | Command, Control, Communications and Information |
| CCITT | Consultative Committee for Telephone and Telegraph |
| CCS | Common Channel Signalling |
| DSTO | Defence Science and Technology Organisation |
| DTMF | Dual Tone Multifrequency |
| ETSI | European Telecommunications Standard Institute |
| GVNS | Global Virtual Network Service |
| ICCV | International Credit Card Validation |
| IN | Intelligent Network |
| IP | Intelligent Peripheral |
| ISDN | Integrated Services Digital Network |
| MLPP | Multilevel Precedence and Pre-emption |
| OSI | Open Systems Interconnection |
| PABX | Private Automatic Branch Exchange |
| POTS | Plain Old Telephone Service |
| SCP | Service Control Point |
| SM | Service Manager |
| SSP | Service Switching Point |
| STP | Signal Transfer Point |
| TINA | Telecommunications Information Networking Architecture |
| TINA-C | TINA Consortium |
| TMN | Telecommunications Management Network |
| UPT | Universal Personal Telecommunications |
| VFN | Vendor Feature Node |
| VPN | Virtual Private Networks |

## 2 CCITT Terminology

| | |
|---|---|
| BCP | Basic Call Process |
| CCAF | Call Control Agent Function |
| CCF | Call Control Function |
| CS1 | Capability Set 1 |
| FE | Functional Entity |
| FEA | Functional Entity Action |
| INAP | IN Application Protocol |
| PE | Physical Entity |
| POI | Point of Initiation |

| | |
|---|---|
| POR | Point of Return |
| SCF | Service Control Function |
| SDF | Service Data Function |
| SF | Service Features |
| SIB | Service Independent Building Block |
| SRF | Specialized Resources Function |
| SSF | Service Switching Function |

## 3 Advanced Intelligent Network

| | |
|---|---|
| AIN | Advanced Intelligent Network |
| AMA | Automatic Message Accounting |
| AOS | Area Of Service |
| ASC | AIN Switch Capabilities |
| ASLP | Administrative SLP |
| FSLP | Feature SLP |
| IM | Information Management |
| MVIF | Multi-Vendor Interaction Forum |
| NA | Network Access |
| NAP | Network Access Point |
| NDC | Network Data Collection |
| NE | Network Element |
| NTM | Network Traffic Management |
| OA | Operations Application |
| OS | Operations System |
| OSLP | Operations SLP |
| P&E | Planning and Engineering |
| RCEE | Resource Control Execution Environment |
| RSA/WFA | Repair Service Answering, and Work and Force Administration |
| SA | Service Assistance |
| SL&C | Service Logic and Control |
| SLEE | Service Logic Execution Environment |
| SLP | Service Logic Program |
| SN | Service Nodes |
| SN&M | Service Negotiation and Management |
| SNEE | Services Node Execution Environment |
| SP | Service Provisioning |

# 1 INTRODUCTION

Intelligent Networks (IN's) are "service-independent" architectures [AIN90] that support services associated with electronic communications, entertainment and information exchange. The term *value added* is used to describe such services due to the great impact they have on human interaction within an electronic environment. They belong, literally, to that class of functions that are added to a network already displaying enormous communications functionality, and which are the most immediately perceptible and of greatest utility to its human users. In other words, an Intelligent Network supports those services that are most valued by human users of electronic communications systems, while avoiding a structure that is in any way specific (i.e. tailored) to such services.

This key characteristic of IN technology is a result of having developed within a climate of rapid technological, regulatory, and market changes; where:

> These changes involve the increased use of network elements that are controlled by or interface with software, a desire to share data and distribute application processing among network elements, the need for standard interfaces between network elements, and user demands for more sophisticated telecommunications services and rapid delivery of services [GAR93].

As a consequence, Intelligent Networks are readily extensible/configurable in response to changing human needs, technical innovation, new telecommunications regulations and emerging markets.

# 2 EMERGING "INTELLIGENCE"

As luck would have it, our aim of better understanding IN technology is hampered at the outset by the inappropriateness of the term "intelligent network" - something of a misnomer, the term owes more to marketing psychology than to common sense. The history of IN technology has made no real claims to "intelligence", in the sense for example that artificial intelligence systems might be said to be intelligent by virtue of learning algorithms, or expert systems by virtue of the encapsulation of human knowledge. A typical framework within which the evolution of IN is analysed is that of [FIS92], where intelligence is simply equated with sophistication and complexity. That recent IN developments include the use of expert system technology [DUN91], does little to change the basic characteristics of IN as a highly complex information technology system. In other words, Intelligent Networks have always been complex, but only in recent times have they shown signs of any "intelligence" - and in any case, the extent to which they are implemented around machine intelligence does little to change the basic underlying concepts of IN technology. Therefore, while "intelligent network" serves as an industry standard term, we need to keep sight of the technologies that are embraced by the concept if we are to avoid the marketing romance to see IN for what it really is.

An oft-cited example of recently implemented IN functionality is AT&T's "800 Service", where "the dialed number is not the network address of the terminating line. Rather, the dialed number is used as an index into a database that contains the terminating line network address" [VER90]. Furthermore, this system allows users (corporate customers in particular) to "specify a different geographic location for the call to terminate at, depending on the location of the calling customer, time of day, or day of the week" [VER90?2]. The wider IN project however, aims to make services such as these readily available to all users (domestic, corporate and military alike), with the promise also that they support affordable and dynamic reconfiguration. For example, as a domestic customer, I might like to visit an aunt in another state and to program (or have programmed for me) my telephone number such that calls from my home state terminate at my home answering machine,[1] while calls from my aunt's state terminate at my aunt's place. Some of the services planned for the future will be familiar to present users of modern PABX systems; for example: Calling Number Identification, Call Tracing, Call Charge Advice, Selective Call Rejection, Direct Dial-in, Selective Call Forwarding, Call Waiting Signal, Closed User Groups, Call Transfer and Private Numbering [DUN91]; while others herald a completely new mode of telecommunications, such as: freephone, universal number, televoting and opinion polling, credit card calling, virtual private network and personal telephony [VAC89].

# 3 IN BUILDING BLOCKS

Intelligent Network architectures are recognisable by certain key elements that are central to the IN concept; specifically: Service Switching Point (SSP); Signal Transfer Point (STP); Service Control Point (SCP); Service Manager (SM); Intelligent Peripheral (IP); and Vendor Feature Node (VFN). These components can be thought of as the building blocks of Intelligent Networks - they are interconnected (typically as shown in figure 1) to form the physical structure upon which the functional architecture is built.

A basic feature of the IN concept is the separation of service control from traditional call processing functions. This is achieved through the use of a small number of centralised database systems (i.e. SCP's) that contain the logic of the network services and control the call processing of the telephone exchanges (i.e. the SSP's) [POP92]. Figure 2 shows how the operation of an Intelligent Network is based on an interaction between SSP and SCP elements (communicating via a signalling network comprising STP elements), where the former initiates an inquiry and the latter responds with a reply. This client-server relationship has an SCP serving a distribution of SSP elements to provide support for calls that invoke IN functionality, and is in turn controlled and configured by an SM element.

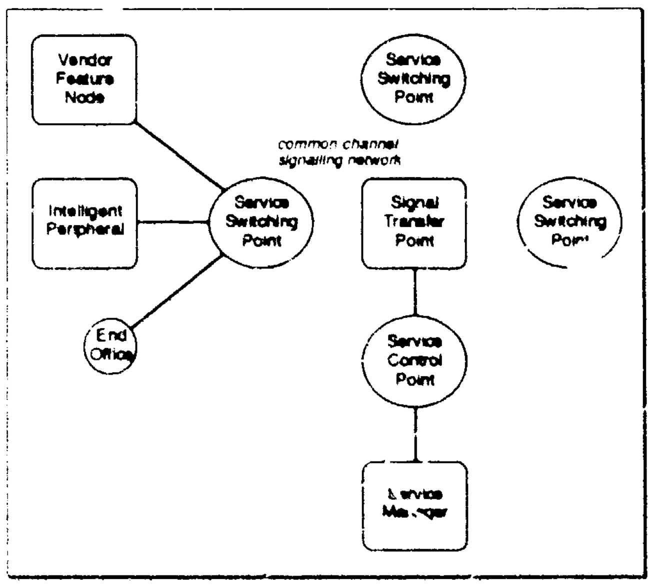
## 3.1 Service Switching Point

Beginning with a crude definition of a Service Switching Point we have: "a jargon term for a modern digital circuit-switching exchange upgraded for intelligent networking, and thus capable of handling the standard CCS#7 signals" [FIS92] - which is to say that the Service Switching

[1] Better still, IN would allow me to dispense with an answering machine altogether by providing me with voice storage facilities (known as "voice-mail"). The type of scenario described here comes under the heading of "personal telephony".

Point behaves like a local switching exchange[2] and serves as the user's access point to the Intelligent Network [POP92]. The switch analyses the user input to determine whether it is capable of providing the service requested - if not fully capable, it forwards the request to the Service Control Point (via the common-channel signalling network) to determine how the call should be handled [VER90].

Another way of thinking of the Service Switching Point is as "software in a switching system capable of recognizing a trigger condition for an IN service" [BEA89]. Here, triggers are events that indicate that the call is an IN call, providing the Service Switching Point with the capability to separate basic call control from that of IN-based service control [HUS91]. Typical triggers include prefix digits or address digits to recognise calls for special handling by the Intelligent Network [ROB91].




source: adapted from K. Verma (ed), *ISDN Systems: architecture, technology, and applications*, Prentice Hall, New Jersey, 1990

**Figure 1. Key Intelligent Network elements**

## 3.2 Service Control Point

The importance of the Service Control Point in the Intelligent Network is apparent in descriptions of it as "the main engine" [ROB91] or "the heart" [POP92] of the network, as becomes clear when we begin to look closer at its operation.

When a Service Switching Point finds it necessary to request support from the network, the response involves an interrogation of information stored in databases dictating how the switch is to proceed. Such a database is provided by the Service Control Point: essentially an "on-line", "transaction-processing" database, with a real-time system response time requirement of less than

2 An SSP may be part of either an end office or an access tandem office [ROB91]. Furthermore, modern switching technology allows the integration of multiple network functions into a single-switching system, such as the combination of SSP, STP, and international gateway functions into a single exchange [KET92]

half a second [ROB91]. The Service Control Point serves the function of responding to a query from the switch by executing service logic that has been customised for a specific subscriber or application, and subsequently sending instructions to the switch on how to continue call processing [HUS91], [FIS92]. The process aims to establish outcomes such as circuit-switched connections from the user to: another user local to the switch, "an interexchange carrier", or to "a service vendor system" (i.e. an Intelligent Peripheral) [VER90].

The role of the Service Control Point is such that its contribution to the Intelligent Network comprises the simplification of: service implementation, network administration, feature changes and updates of service provider records [POP92]. Towards these ends, Service Control Point's are designed to accommodate the addition of: processing power, memory, or new software without causing any disruptions to the service [ROB91]. In fact, the Service Control Point potentially coincides with a highly sensitive single point of failure which encourages the incorporation of fault-tolerance in its internal design [ROB91]. Likewise, Service Control Point's are typically deployed in a "mated-pair" configuration, with each node containing identical user records [HUS91].

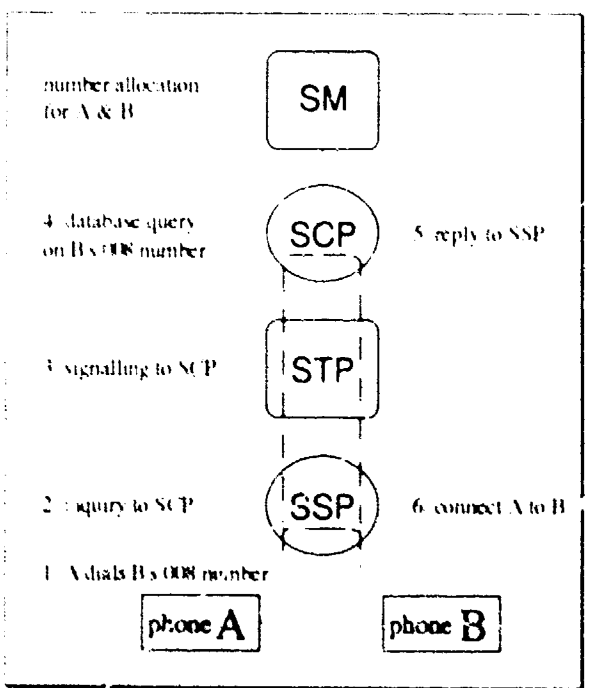



Figure 2. Operation of the Intelligent Network

## 3.3 Signal Transfer Point

Signal Transfer Point's are packet switching nodes on the common channel signalling network (viz CCS No. 7). These nodes "know where to look for information", and so act as routers between SCP databases and SSP switches [FIS92]. Signal Transfer Point's are very high-capacity switches, as they are required to terminate a large number of signalling links, perform a great deal of protocol processing, and route a high volume of messages through their links [ROB91]. As with the Service Control Point, the potential for the Signal Transfer Point to become a

disastrous single point of failure is grounds for requiring these packet switches to be very reliable. Typically, they are deployed in "geographically separated pairs", so that in the event of a disaster total traffic volume can be handled by the second site [ROB91].

## 3.4 Service Manager

The human interface for operating personnel and users to specify services is provided by the Service Manager. This serves as the central network interface for both the service provider and the service subscriber [HUS91]: supporting the interactive processing and updating of user records by operations personnel, and offering the user with an interface to the centralised databases in the Intelligent Network [ROB91]. The interface follows a paradigm according to which basic service capabilities are linked to define specialised user services - providing also the mechanism for constructing the databases that control the real-time connection functions of the service [VER90].

The Service Manager interacts closely with the Service Control Point to implement and control service provisioning by maintaining the network database [FIS92], [BEA89]. It fulfils this role via management software and information databases that load, administer and maintain call processing information at the Service Control Point [FIS92]. In other words, features of the Service Manager include: supervision, remote operations and maintenance of Service Control Points, and co-ordinated software downloading [POP92].

## 3.5 Intelligent Peripheral

The Intelligent Peripheral provides service assistance for appropriate IN calls. It executes this role by offering telecommunications capabilities, such as announcements and Dual Tone Multifrequency (DTMF) digit collection [VER90], and perhaps also advanced functions such as voice recognition or language translation [BEA89], or the facility to prompt the caller to further direct the routing of the call by asking for additional information [HUS91].

An Intelligent Peripheral is connected to a Service Switching Point and operates under its control, or alternatively under the control of a Service Control Point. The economic advantage of this network element is that it allows several users to share peripheral services without having to implement these in all Service Switching Point's [POP92].

## 3.6 Vendor Feature Node

Where services are distributed which are not integrated in the Intelligent Network, a special network element is required, known variously as a Vendor Feature Node [VER90], or an Adjunct [AIN90]. The Vendor Feature Node is interconnected with a Service Switching Point and is accessed by the user through the switch. The Vendor Feature Node need only be designed to have the capacity and characteristics required for a particular service, and not all the other services that the Service Switching Point software and hardware provide [VER90].

# 4 BELLCORE'S ADVANCED INTELLIGENT NETWORK

Bellcore's Advanced Intelligent Network (AIN) can be seen as the next phase of development after IN/1, which introduced the concept of centralised databases and offered the means of introducing new services in a ubiquitous fashion and with operational uniformity. With AIN, rapid and customised development is now possible by virtue of the concept of "functional blocks" which allows nonprogrammers to easily create new services by writing a script known as a Service Logic Program (SLP) [POP92], [ROB91].

The AIN system is of great importance to us in our aim to better understand the IN concept in general, and IN architectures in particular, simply because of the huge impact Bellcore has had in the development of this technology. To date, much of the technical literature on IN has borrowed heavily from Bellcore's architectures (which include IN/1, IN/2, IN/1+, and finally AIN), or at the very least, has adopted the language coined by Bellcore. The impact of Bellcore has not only been technical but also economic due to the backing of telecommunications giants such as AT&T and the Bell companies (i.e. the Bellcore Client Companies). In this way, market forces ensure that the latest IN architecture from Bellcore serves as a defacto standard[3].

A presentation of the main concepts of AIN, as summarised from [AIN90], appears as an appendix.

# 5 STANDARDISATION

Responsibility for the standardisation of IN has been accepted by CCITT (SG XI) since 1991. In particular, the CCITT Q.1200 series of recommendations discuss the Intelligent Network in terms of a *Capability Set* continuum, of which Capability Set 1 (CS1) marks the state of work to date. The intention is for CS1 to define "the scope and content of INs for the near term without curtailing subsequent growth"; providing the telecommunications industry with a usable set of recommendations that will enable the "low-risk introduction" of a wide range of advanced services, along with the capability for rapid service delivery and customisation [DUR92]. A list of the relevant recommendations is given in table 1.

## 5.1 Objectives

The objectives which IN technology must satisfy are defined by CCITT in response to "demands made by the operating companies for increased responsiveness to customer needs", and comprise [DUR92]:

- "increase service velocity" - i.e. enable the rapid introduction of new services in response to market forces

- encourage a broader range of services (e.g. information services, broadband and multimedia bearer capabilities)

[3] Industry support has in fact broadened of late with the advent of the Multi-Vendor Interaction Forum (MVIF) which will provide the co-operative development environment for AIN.

- support multivendor competition and consistent integration across several vendors' equipment
- support the evolution from existing networks with the capability of interworking between deployed technology and existing networks

**Table 1. CCITT Q.1200 series recommendations**

| *code* | *description* |
|---|---|
| Q.1201 | principles of intelligent network architecture |
| Q.1202 | intelligent network service plane architecture |
| Q.1203 | intelligent network global functional plane architecture |
| Q.1204 | network distributed functional plane architecture |
| Q.1205 | intelligent network physical plane architecture |
| Q.1208 | general aspects of the intelligent network application protocol |
| Q.1211 | introduction to intelligent network Capability Set 1 |
| Q.1213 | global functional plane for intelligent network Capability Set 1 |
| Q.1214 | distributed functional plane for intelligent network Capability Set 1 |
| Q.1215 | physical plane for intelligent network Capability Set 1 |
| Q.1218 | interface recommendations for intelligent network Capability Set 1 |
| Q.1290 | vocabulary of terms used in the definition of intelligent networks |

source: Mike Lai, *Interoperability Issues in Connection with the Use of High Speed Networks*, unpublished, Defence Science and Technology Organisation, 1993.

## 5.2 Characteristics

An IN architecture is specified by CCITT with the aim of realising the objectives listed above - the characteristics of which comprise [DUR92]:

- extensive use of information processing techniques and network resources
- integration of service creation and implementation by means of reusable standard network functions
- flexible allocation of modularised and reusable network functions among physical elements
- standardised communications between network functions via service-independent interfaces
- service provider access to the process of composition of services through the combination of network functions
- service subscriber control of subscriber-specific service attributes in terms of definition and deployment
- standardised management of service logic

## 5.3 Service Types

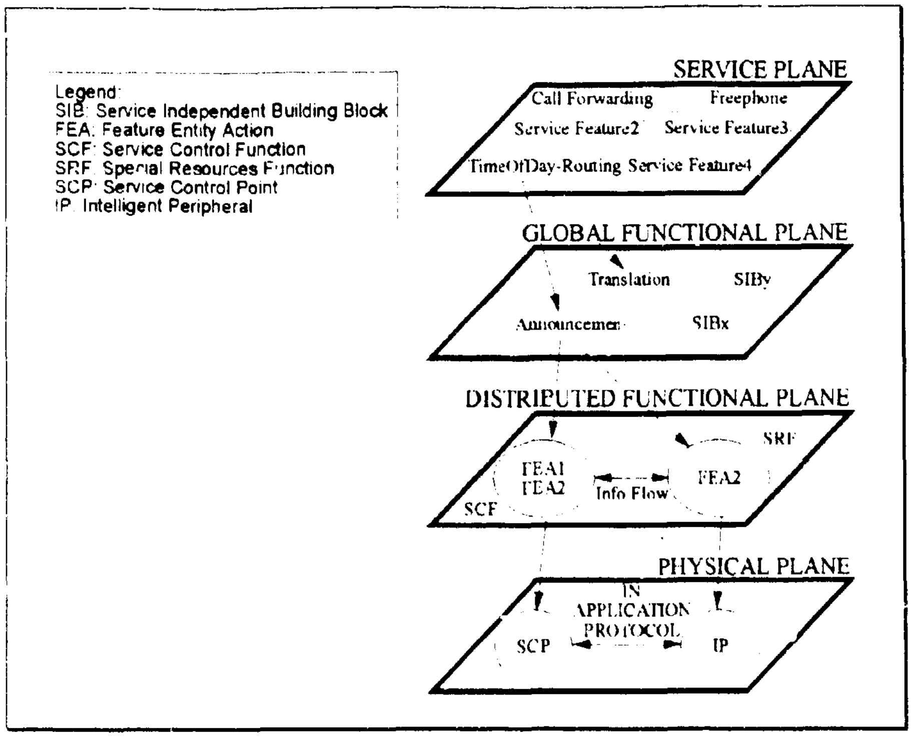
IN services are categorised by CCITT according to two types; viz. Type A and Type B [DUR92]. Type A is addressed by CS1 and has the advantage that it comprises services of "proven value" which are based on "well-understood control relationships between network components". Typically, these services can only be invoked during call set-up or tear down. They have the distinction of being: *single-user*, *single-ended*, *single-point-of-control*, and of *single-bearer* capability. In other words, they do not support: end-to-end messaging or control (i.e. they do not apply to the active phase of the call), interaction between several SLP's, or multi-media. Type B services by contrast can be invoked at any point during a call, and also on behalf of, or with direct impact on, one or more users.

## 5.4 A Conceptual Model

CCITT's draft recommendation Q.1201 defines a model of IN known as the IN Conceptual Model. As shown in figure 3, the model involves four levels of abstraction of the IN concept, referred to as *planes*:

- the Service Plane - an exclusively service-oriented view
- the Global Functional Plane - a view of the different functionalities of the network considered as a single entity
- the Distributed Functional Plane - a view of the distributed functions
- the Physical Plane - a view of the physical network elements

Detailed overviews of the four-plane structure is presented in [WYA91], [GAR93] and [APP93] The Service Plane sits at the most abstract level, being totally independent of the network implementation - i.e. it defines the IN services available to users and their features, yet hides the way in which the service is implemented, and is therefore of primary interest to service users and providers. CCITT recommends that service characteristics be classified and service capabilities identified by decomposing services into Service Independent Building Blocks (SIB's), where "These reusable service independent blocks (such as translation, user interaction or charging) will form the basis for input to global functional plane modelling and distributed functional plane modelling" [CCI93a]. Possible services include: Freephone, Call Forwarding, Virtual Private Networks (VPN), and Universal Personal Telecommunications (UPT). The model for this functional decomposition is the recognition of services as comprising one or more Service Features (SF), where an SF is "the smallest part of a service that can be perceived by the user", and where "These SF's can also be used as building blocks in the specification and design of new, more complex services". Furthermore, SF's comprise one or more SIB.



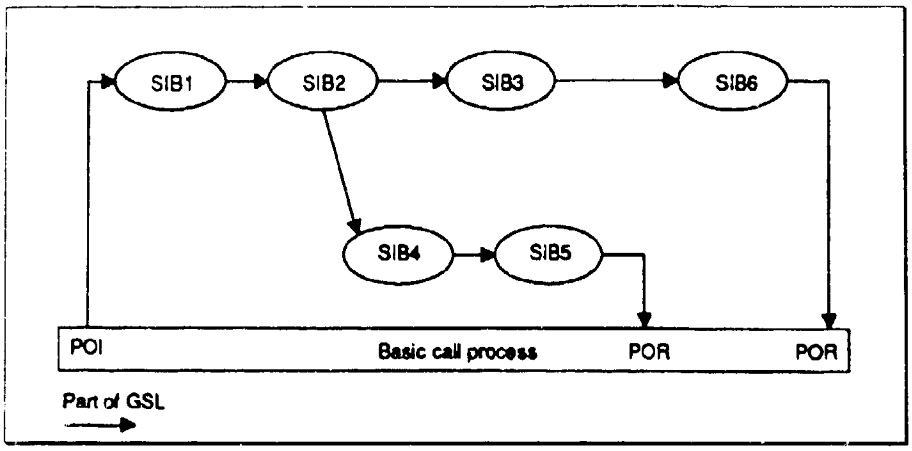

source: José M. Duran and John Visser, "International Standards for Intelligent Networks", *IEEE Communications Magazine*, vol. 31 no. 2, February 1992, pp. 34-42.

**Figure 3. CCITT IN conceptual model**

The Global Functional Plane is of primary interest to service designers and is defined by SIB's and the call-processing model (as encapsulated in a special SIB called the Basic Call Process, BCP). Here, service-specific logic combines SIB's to create new services unique to a particular user or network operator. The idea is that the Global Functional Plane maps SF's onto one or more SIB's, such that service and SF specific functions are "redefined in terms of the broad network functions required to support them" [CCI93b]. Similarly, each SIB is mapped onto one or more Functional Entity (FE) in the Distributed Functional Plane. The service independent characteristic of an SIB is manifest in the fact that it has no "knowledge of subsequent SIBs". However, there exists one entity in this plane that does have service-specific dependence and that is the Global Service Logic (GSL) which controls the way SIB's are interconnected (as patterns of "chains" and "branches") to form SF's. As shown in figure 4, the GSL is also responsible for controlling the interaction between the BCP and the SIB chains via two interfaces known as the Point of Initiation (POI) and the Point of Return (POR). In this way, a Service Feature is defined by a "pattern" of standard SIB's; such as from the fourteen SIB's defined for CS1: algorithm, charge, compare, distribution, limit, log call information, queue, screen, service data management, status notification, translate, user interaction, verify, and basic call process [GAR93].

The Distributed Functional Plane, of primary interest to network designers, deals with FE's and Functional Entity Actions (FEA's). This view of the Intelligent Network has it categorised according to logical functional entities (i.e. FE's) that have associated with them distinct actions

(i.e. FEA's). The network capabilities of a given SIB then, are performed by grouping FEA's across one or more FE under the co-ordination of information flow.




source: CCITT Recommendation Q.1203 - Intelligent Network - Global Functional Plane Architecture, ITU, 1993.

**Figure 4. Global functional plane model**

The Physical Plane deals with the functions and communications protocols of Physical Entities (PE's), where each PE consists of one or more FE. This plane, therefore, is of primary interest to network operators and equipment providers.

Based on this model, a framework of IN emerges which consists of two architectures: one functional and the other physical - related to one another by the mappings of functional to physical entities within the network. However, it is the functional architecture that distinguishes IN because "it is at that level that the relationships between service logic and call processing can be recognised" [DUR92].

## 5.5 A Functional Architecture

In line with the focus of IN capability set CS1 on service processing, the functional architecture (refer to figure 5) encompasses: end-user access to call and service processing; service invocation and control; and end-user interaction with service control [GAR93]. A Functional Entity called the Call Control Agent Function (CCAF) provides an interface whereby a user may access the call and service processing offered by a CS1 Intelligent Network. The CCAF in turn interacts with call control, so that through the combined action of the Call Control Function (CCF) and the Service Switching Function (SSF), the user is able to request an IN service. Here, the current call processing infrastructure of existing digital exchanges provides the appropriate functionality on which to build; viz. call control's Basic Call State Model (BCSM) which supports the processing of basic two-party calls. Added to this is the SSF which detects when IN logic is to be invoked; and when this is the case, the SSF interacts with the Service Control Function (SCF) which in turn processes the appropriate IN logic. Furthermore, call control and service switching are augmented with specialised resources associated with interactions between the end-user and the Intelligent Network, such as pre-recorded announcements, DTMF, and other intelligent

peripheral functions. Such resources are managed by a Functional Entity called the Specialized Resources Function (SRF). The SCF may respond to the invocation of IN logic by requesting the CCF and SSF to perform call and connection processing such as routing or charging. The SCF may also request these service invocation functions to establish a connection between a user and an SRF. Furthermore, in performing related service data processing, the SCF may also draw on database services from the Service Data Function (SDF) such as data retrieval and updating.

As shown earlier, functional entities such as those we have been considering here are defined as part of the Distributed Functional Plane, where the relationships between Functional Entities define the information flows from one entity to another. Furthermore, these relationships determine the grouping of Functional Entity Actions required to implement the network capabilities of a given SIB.

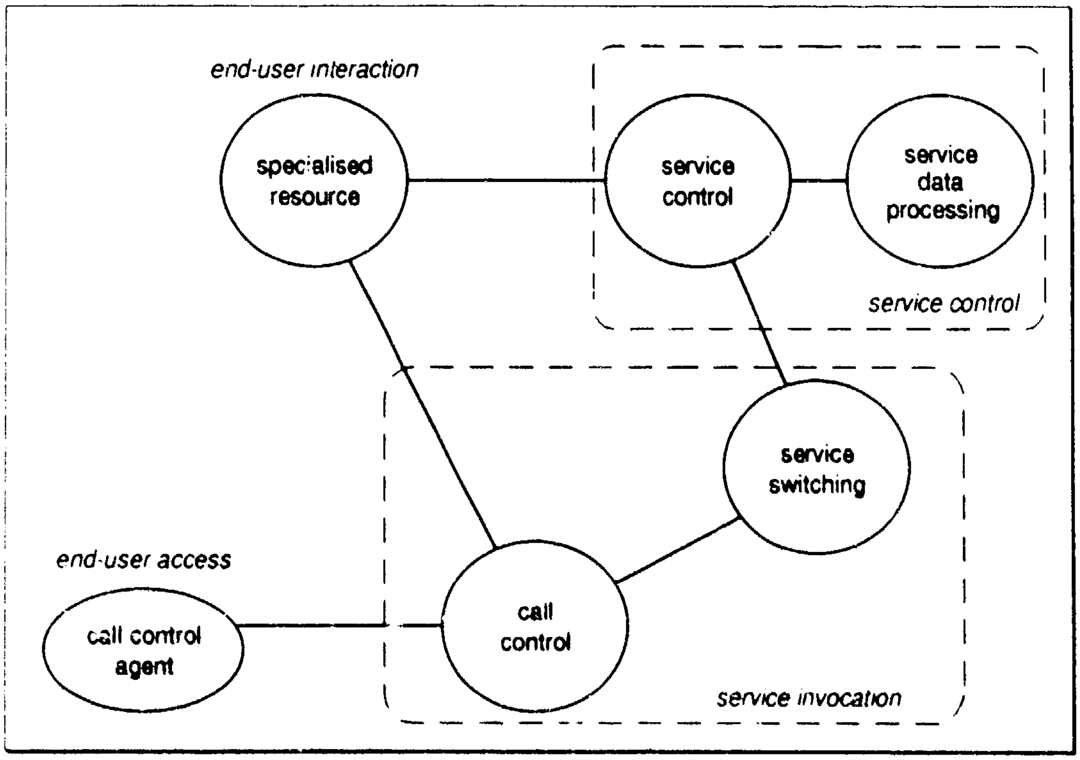



**Figure 5. CS1 functional architecture**

## 5.6 A Physical Architecture

We have seen also that the Physical Plane relates to the Distributed Functional Plane by implementing Physical Entities around one or more Functional Entities. In the CS1 physical architecture for example, a Service Control Point is built around an SCF and an SDF, while an Intelligent Peripheral is based solely on an SRF [GAR93]. This is one aspect of the mapping of distributed functional plane to physical plane elements. Another issue is the way that information flows between Functional Entities impact on the specification of the signalling messages between Physical Entities. The need for a physical mechanism with which to carry functional entity

information is realised in the form of an application layer protocol,[4] known in CS1 as the IN Application Protocol (INAP). Specifically, INAP supports the mapping of the entities SSF, SCF, SDF, and SRF to Physical Entities. This protocol is in turn supported by "lower layer" protocols such as the Common Channel Signalling system SS7, or the Basic Rate and Primary Rate Interface (BRI, PRI) used in the Integrated Services Digital Network (ISDN).

The physical architecture defines, therefore, the process whereby functional entities and the information flow interdependencies between them map into physical entities and protocol interfaces.

## 5.7 Limitations

The current CCITT specification for IN has certain limitations:

> The IN CS-1 architecture and interfaces are a subset of the target IN architectures and interfaces, and therefore do not address all possible IN goals and objectives. In particular, IN CS-1 focuses on service processing requirements in support of the target IN CS-1 services. It does not address requirements for service creation, service management, and network management. It is expected that these latter requirements will be addressed by nonstandard solutions for IN CS-1, as driven by market forces. Future capability sets may address standard solutions in these areas [GAR93].

Furthermore, with CS1 restricted in scope to the SSP/SCP interface, the standards are insufficient on their own for the implementation of a complete network [HIL93]. Along with the ambiguity of the CS1 standards, this makes for a situation where incompatibilities between different vendors may arise. In recognition of this problem, the European Telecommunications Standard Institute (ETSI) is working towards a European standard, known as Core Intelligent Network Application Protocol (i.e. Core INAP), that is in effect an unambiguous subset of CS1.

# 6 TINA

As we have seen, the two main architectural specifications serving as flagships for the development of IN technology are the Advanced Intelligent Network from Bellcore and Capability Set 1 from CCITT. The two architectures are closely aligned[5] and are clearly pursuing a common architectural objective [GAR93]. The most significant differences are that AIN addresses service management and network management,[6] whereas CS1 addresses service processing. This raises the topical issue of the

[4] In the *Open Systems Interconnection (OSI) Reference Model* for computer networks the application layer is the highest (i.e. most abstract) in a "stack" of seven protocol layers.

[5] Specifically, it is the near-term releases of AIN Release 1 known as AIN 0.1 (for 1993-1994) and AIN 0.2 (for 1995-1996) which are closely aligned with CS1.

[6] With respect to service management, this comprises the control of data distribution and coherency according to Area Of Service (AOS), such that common service and subscription data is "fractured" around *AOS maps*; and with respect to network management, AIN is largely an extension of existing SS7 management procedures. Yet, while AIN presently places a fairly small load on SS7 infrastructures the service intensive environments of the future herald a requirement for service-specific load management procedures [RUS93].

overlapping boundary between IN architectures and Telecommunications Management Network (TMN) architectures. The pressing need for an integration of these architectures [APP93] is being addressed by a recently created organisation known as the TINA Consortium (TINA-C) which is defining an architecture referred to as the Telecommunications Information Networking Architecture (TINA) [BAR93].

CCITT's Broadband Integrated Services Digital Network (B-ISDN) conceives an interplay of three 'planes', known as the User Plane, Control Plane, and Management Plane. From this point of view, the boundary between IN and TMN corresponds to the boundary between the two latter planes. Accordingly, management functions appear in both planes:

> The control plane relates to the establishment of calls and connections and the resources needed in the node to handle these. This plane deals with the network signalling system(s) used (e.g. SS7, Q93x) and interfaces to the higher level IN services. In alignment with the IN architecture, some of these functions could be part of the IN Distributed Service Logic. The Management plane handles the operational and administrative management side of the node. Primarily, it deals with statistics, status, configuration and fault reporting (alarms). The management plane logically interfaces as a Network Element to the higher order TMN management functions and the network services functions [LLO93].

In other words, whereas the Control Plane, and the intelligent network that interfaces to it, focuses on "service management" [APP93], the Management Plane, and the telecommunications management network that interfaces to it, focuses on what we traditionally think of as telecommunications management; viz. operations and administration.

The imperative for the architectures of IN and TMN to integrate comes from the need to support the interoperability of applications from both architectures.[7] Consequently, it is not possible to support two independent architectures, and similarly, the interconnection of IN and TMN as divergent architectures would be very difficult [APP93]. With the backing of Bellcore in the United States, BT in the United Kingdom, and NTT in Japan, the TINA Consortium has taken upon itself the responsibility for the integration of the two architectures. Furthermore, given the support for TINA from the IN group of ETSI, and the fact that the "ETSI text has been adopted as a starting point for the coming study period of CCITT (1992-1996)" [APP93], we can expect future CCITT recommendations for IN and TMN to be closely aligned.

## 7 GLOBAL INTELLIGENT NETWORK ARCHITECTURES

[KET92] divides the world's various national carriers into three broad categories according to IN capability: (a) full IN capability (along the lines of AIN); (b) partial IN with SSP functionality and/or *switched-based service logic* but not SCP functionality; and (c) non IN, i.e. Plain Old Telephone Service

[7] By way of example, [APP93] refers to the IN application called Freephone, where billing corresponds to accounting applications in TMN.

(POTS). The term "switched-based service logic" refers to IN service logic (including basic number translation but excluding advanced routing features) that is resident in a switch as opposed to a Switch Control Point. Such an implementation implies the existence of multiple databases as opposed to the centralised database configuration that exists with the presence of an SCP element. Therefore, while offering partial IN capabilities, such a network pays the penalty of having to provide relatively high computational resources in its switches, as well as having to deal with the administration and data coherency of multiple databases. However, as [KET92] points out, the partial IN configuration caters for a transition to a full IN architecture with the inclusion of an SCP in place of switched-based service logic.

In the meantime, full IN services may be made available to subscribers to partial IN or non-IN networks by connecting national carriers such as these to a *Regional IN Node*. In this scenario, the Regional IN Node of one country's carrier provides advanced services to its multinational corporate customers located in a region spanning several countries or even an entire continent. Another arrangement described by [KET92] is the *internetworking* of IN networks from different carriers - accomplished by facilitating direct communications between carriers (i.e. SCP to SCP communications) for the purpose of sharing one another's IN features. This has its main applicability with IN services such as Global Virtual Network Service (GVNS) and International Credit Card Validation (ICCV).[8] The introduction of global IN services such as these are justified on the grounds that they "control costs and, at the same time, enhance network management control (e.g., efficiency of operation) and feature functionality" [SYK92], and as a consequence, it is essential that efficient use be made of international transmission facilities.

## 8 THE MILITARY ENVIRONMENT

The military user will be aware of a profound significance in technological capabilities such as those described in the previous sections. The emergence of global intelligent networks in the commercial world opens the possibility of a sophisticated interconnectivity of value added networks managed by various national military organisations. Furthermore, it is now technically feasible for advanced countries with large military resources to establish their own regional IN nodes in order to provide an IN capability for their allies. But just as startling a scenario is the ability of a national military organisation to establish an IN capability by subscribing to IN services provided by a private or public telecommunications carrier. In such a case there is the added choice open to the military as to the design, maintenance and control of value added applications. The nature of IN technology is such that client-operator relationships can accommodate a variety of configurations around service creation and provisioning. Hypothetically, the military might elect to employ an IN operator to install and manage on its behalf a Command, Control, Communications and Information ($C^3I$) system which it has designed or commissioned - reserving for itself the capability to dynamically control the application. Alternatively, intelligent networks would allow the military to introduce and manage sophisticated applications in a highly extensible and configurable manner that would also be cost effective.

8 For the validation of telephone credit cards issued by another county's carrier

### 8.1 A National Defence Force Perspective

In contemplating the adoption of IN technology into its operations the Australian Defence Force (ADF) faces a difficult decision: install ADF-owned "standard" IN firmware in parallel with systems now appearing in the commercial world and public telecommunications carriers; or subscribe to IN services offered by existing IN operators. There is of course a wide middle ground. With the rapid development of IN standards and the emergence of "standard" IN network elements the possibility exists of selectively interconnecting with the IN systems of domestic private and public organisations, as well as those of allied military organisations. In any case, as Rear Admiral K A Doolan points out, the adherence to standards (for strategic communications at least) has a more fundamental importance:

> In the past Defence has invested heavily in developing unique capability solutions and fostering military standards for most communications capabilities. We recognise that globally, civil industry is now setting the pace in communications standards. Therefore Defence is committed to the adoption of emerging national and international standards for communications wherever possible. Defence will also continue a commitment to open systems architecture wherever possible [DOL93].

Implicit in this statement is the catch-cry of the times: "technology for affordability", and the wide-spread recognition that open systems[9] engender not only technical flexibility but also the purchasing power associated with an ongoing choice[10] of vendors.

Also, subscription to telecommunications facilities on offer by the civil infrastructure has problems of its own - this strategy being efficacious only in the event that such systems meet the unique requirements of military communications, such as Multilevel Precedence and Pre-emption (MLPP). IN provides a means of "militarising" the civil infrastructure in a fairly flexible and cost-effective manner: military attributes would in effect be "added on", or "plugged in", to existing commercial telecommunications systems. This would be the responsibility of the public carrier and would be achieved by designing IN services around military attributes - for example, MLPP might be offered as an IN service.[11]

To a large extent, IN is a young technology waiting to be put to good use, and it is quite possible that the ADF's unique requirements as a user of telecommunications will see it look more to IN in the future; especially as the cost of communications becomes harder to sustain and pressures mount to realise greater interoperability with systems in the civil infrastructure and in other countries. Of course, doctrinal and security implications may well outweigh the technical and economic issues we have considered so far - a discussion of which is beyond the scope of this paper.

9 Systems adhering to international non-proprietary technical standards.

10 The power to choose vendors, that is, that continues throughout the life of the communications system, in contrast with the scenario of being "locked in" to one particular vendor once the initial purchasing decision has been made.

11 As a matter of fact, Telecom Australia is conducting research into this area at the time of writing

## 8.2 An International Allied Perspective

With the relaxation of Cold War hostilities and the emergence of Third World powers as a perceived political threat in the West, many military forces and defence industries are undergoing dramatic changes to their organisations and activities [DOO93]. The US, for example, is displaying "a trend toward intertwining and balancing [of] commercial and government business" [CUR93]. Consequently, the growing political and economic pressures in the developed world on its military budgets is placing increasing value on the capability of integrated allied military operations, as well as a greater focus on the problematic rationalisation of national resources for military purposes. These dual processes translate into the technical issue of interoperability of military communications with allied systems and the systems of domestic private and public telecommunications operators. Not only are areas such as physical transmission and communications protocols affected but also the areas closest to the end user, including the very applications that the communications systems are designed to support. The significance of IN in this context is that the technical means are provided for value added services to be created, provided, and controlled in a manner that is independent of the configuration of the underlying communications infrastructure - the technical means, that is, for interoperability of allied military applications.

In response to the dual forces of changing world markets and international political boundaries the US is reconsidering its military role. Consequently, with a military budget that is fast becoming unsustainable both economically and politically the US has responded by making its military technological development more focused:

> DOD has announced seven major technological thrusts: global surveillance and communications; precision strike; air superiority and defense; sea control and undersea superiority; advanced land combat; synthetic environments; and technology for affordability [CUR93].

The communications response to this policy is the architecture known as *Global Grid* [MAC93]. The underlying concept involved here is that of a global communications capability that has the form of an international grid of interconnected communications networks. Potentially, individual networks (referred to as *crystal islands*) will be of extremely high capacity. Furthermore, the networks, though interconnected and therefore necessarily interoperable, retain a high degree of autonomy. At a national level a given network may correspond to one of the US military services, while at an international level a network may correspond to the communications resources committed by one of the US's allies. Naturally, the intended integration of "tri service" communications is far greater than that envisaged between allied networks; the latter (it would seem) intended for integration only in response to special circumstances, such as a UN "peace-keeping" action. The tactical motivation at play here is the capability of prosecuting a "precision strike" anywhere in the world - and to have the added capability of doing so as a combined allied operation.

There are also great advantages in Global Grid for allies of the US such as Australia. The potential to "tap in" to the huge communications resources of the US military by judiciously

committing a subset of one's own military network (either permanently or on a needs basis[12]) may have certain attractions for the ADF. As already mentioned, Global Grid is premised on communications interoperability, where IN technology will support applications interoperability. Perhaps the most important application that will be provided via an intelligent network on a Global Grid is $C^3I$. The technical possibility exists, therefore, for participants of Global Grid to access in real-time the military sensors of other countries, while simultaneously controlling access to one's own sensors according to the dictates of policy.

12 The reader is referred to the research and development at the Defence Science and Technology Organisation (DSTO) into "policy-based gateways" which is being conducted under a memorandum of understanding with the US.

## REFERENCES


AIN90 *Advanced Intelligent Network: Release 1, Network and Operations Plan*, Bell Communications Research, Special Report SR-NPL-001623, Issue 1, June 1990.

APP93 Menso Appeldorn et al., "TMN + IN = TINA", *IEEE Communications Magazine*, March 1993, pp. 78-85.

BAR93 William J. Barr et al., "The TINA Initiative", *IEEE Communications Magazine*, March 1993, pp. 70-6.

BEA89 Art Beaty, Jr., "The Evolution to Intelligent Networks", *Telecommunications*, February 1989, pp. 29-36.

CCI93a CCITT Recommendation Q.1202 - Intelligent Network - Service Plane Architecture, ITU, 1993.

CCI93b CCITT Recommendation Q.1203 - Intelligent Network - Global Functional Plane Architecture, ITU, 1993.

CUR93 Malcolm R. Currie, "Expert Opinion: Peace is transforming aerospace and military industries", *IEEE Spectrum*, January 1993, pp. 72.

DOL93 K. A. Doolan, "Blue Skying for Year-2000 Defence", *Defence Industry & Aerospace Report*, vol. 12 no. 9, June 1993, pp. 4-12.

DOO93 Dave Dooling, "Aerospace and military", *IEEE Spectrum*, January 1993, pp. 72-5.

DUN91 Mitchell Duncan, "Expert Systems in the Intelligent Network", *Australian Communications*, April 1991, pp. 61-68.

DUR92 José M. Duran and John Visser, "International Standards for Intelligent Networks", *IEEE Communications Magazine*, February 1992, pp. 34-42.

FIS92 Stewart Fist, "Make Way For the Intelligent Network", *Australian Communications*, May 1992, pp. 57-65.

GAR93 James J. Garrahan et al., "Intelligent Network Overview", *IEEE Communications Magazine*, March 1993, pp. 30-6.

HIL93 Tim Hills, "How Advanced is the Advanced IN?", *Communications International*, July 1993, pp. 52-4.

HUS91 S. S. Husain et al., "IN Architectures", *Communications International*, September 1991, pp. 83-92.

KET92 Herbert W. Kettler et al., "AT&T's Global Intelligent Network Architecture", *AT&T Technical Journal*, vol. 71 no. 5, September/October 1992, pp. 30-5.

LAI93 Mike Lai, "Interoperability Issues in Connection with the Use of High Speed Networks", unpublished, Defence Science and Technology Organisation, 1993.

LLO93 Alan Lloyd, "Service and Management Aspects of B-ISDN Systems", *Proceedings from Australian Broadband Switching and Services Symposium 1993*, July 1993, pp. 354-62.

MAC93 Dan McAuliffe, "ATM Networking: Early Trials", *Proceedings from ATM Networking for the Late 1990's*, April 1993.

POP92 R. Popescu-Zeletin and T. Magedanz, "Applying Open Network Provision to ISDN and Intelligent Networks", *Computer Networks and ISDN Systems*, no. 24, 1992, pp. 1-14.

ROB91 Richard B. Robrock, "The Intelligent Network - Changing the Face of Telecommunications", *Proceedings of the IEEE*, vol. 79 no. 1, January 1991, pp. 7-20.

RUS93 Peter A. Russo et al., "IN Rollout in the United States", *IEEE Communications Magazine*, March 1993, pp. 56-63.

SYK92 Jack Sykes and Eldred J. Visser, "Globalization of Intelligent Network Services", *AT&T Technical Journal*, vol. 71 no. 5, September/October 1992, pp. 6-12.

VAC89 X. du Vachat et al, "Services Offered by Intelligent Networks", *Electrical Communication*, vol. 63 no. 4, 1989, pp.331-6.

VER90 K. Verma (ed), *ISDN Systems architecture, technology, and applications*, Prentice Hall, New Jersey, 1990.

WYA91 George Y. Wyatt et al., "The Evolution of Global Intelligent Network Architecture", *AT&T Technical Journal*, vol. 70 no. 3-4, Summer 1991, pp. 11-25.

# APPENDIX A

# GENERAL SUMMARY OF AIN

## A.1 General Definitions

### A.1.1 Network Systems

Network Elements (NE's) primarily perform *call processing* functions.

Operations Systems (OS's) primarily perform *operations* functions.

### A.1.2 Automated Services

Service management support is provided through the mapping of *service views* into *network views* and vice versa. That is, a subscriber's AIN service is mapped to all of the NE's that provide the service. In this way, the details of the implementation of services across the network systems is hidden from both the subscriber and service manager.

### A.1.3 Data

AIN incorporates a *common data model* which is designed to allow applications to share common data without replication. This guarantees data consistency; that is, interfaces between OS's and NE's have a consistent *data view*.

## A.2 Architecture

Two views of the AIN architecture are: a functional view and a physical view. The former consists of *functional groups* and Operations Applications (OA's). The latter is an implementation of the functional groups into network systems.

### A.2.1 Functional

Functional groups are created by Functional Entities (FE's). Together, FE's and OA's form the *operations functions* of the architecture, defined as a set for each *operations domain*.

#### A.2.1.1 Entities

Seven FE types are defined, viz.:

- Network Access (NA)

The entry point for *functional users* - i.e. "an entity external to the functional architecture that uses the functional architecture capabilities to exchange information with other functional users". Here detected *access events* (information type on the functional user and NA FE interface) are translated into *uniform messages* (information type between FE's).

- Service Switching (SS)

These are functions providing "generic call processing capabilities" used by SL&C FE in the provision of AIN services. Using a model of "basic call

processing for a two-party call", known as the Basic Call State Model (BCSM). The SS FE maintains a *connection view* of call connections created by it. In this way, uniform messages from the SL&C FE result in connections being controlled by the SS FE. It responds to *trigger* information originating from an NA FE or IM FE. The connection view and state information is exported to SL&C FE.

- Service Logic and Control (SL&C)

On invocation from SS FE, SLP's are executed by SL&C FE to perform programmed activities such as call routing. Using data from IM FE, the SL&C FE invoke as well as provide functional support for: Administrative SLP (ASLP), Feature SLP (FSLP) and Operations SLP (OSLP).

- Information Management (IM)

These functions guarantee *information persistence* through the manipulation of *permanent data objects* defined by *data templates*.

- Service Assistance (SA)

These functions control "abstractions of physical entities" (e.g. voice synthesisers) known as *functional resources*, in order to exchange information with functional users.

- Automatic Message Accounting (AMA)

The AMA FE perform *record level correlation* through the organisation of data into single records which they also format and deliver to billing entities in OS's. The desired format of records is determined by commands from the SL&C FE. Data involved in the record level correlation, formatting and delivery are sent to the IM FE for storage.

- Operations (OP)

These are real-time functions associated with the *local operations*: memory administration, surveillance, testing, traffic management, and data collection. Furthermore, OA functions are also supported, such as: control of alarms, status requests etc. via the OA; event detection and reporting control via other FE; and organisation of persistent data for the OA.

### A.2.1.2 Relationships

Three types of relationships exist:

- Control

Control relationships exists between FE's.

- User Access

User access relationships exist between functional users and the NA FE.

- Transport

The transport relationship exists between two functional users, or between a functional user and the SA FE.

### A.2.1.3 Groups

The four functional groups defined in AIN are:

- AIN Switch Capabilities (ASC)

Based on the NA, SS, IM, SA, and OP FE, the ASC enables an AIN Switching System to identify calls associated with AIN services, detecting whether conditions for service involvement are met, and where they are, initiating a dialogue with the SLEE. In this way, the ASC requests and responds to call processing instructions from the SLEE.

- Service Logic Execution Environment (SLEE)

Based on the SL&C, IM, AMA, and OP FE, the SLEE appears in Service Control Points (SCP's) where it performs operations that administer and maintain services.

- Services Node Execution Environment (SNEE)

This is implementation specific and is not defined in AIN, though it may be similar to the SLEE. In any case, SNEE appears in Service Nodes (SN's) where it operates similar to a SLEE, receiving messages from the ASC, executing SLP's, and issuing messages to the ASC.

- Resource Control Execution Environment (RCEE)

Based on the SA, IM, and OP FE, the RCEE appears in the Intelligent Peripheral (IP) and SN.

### A.2.1.4 Domains

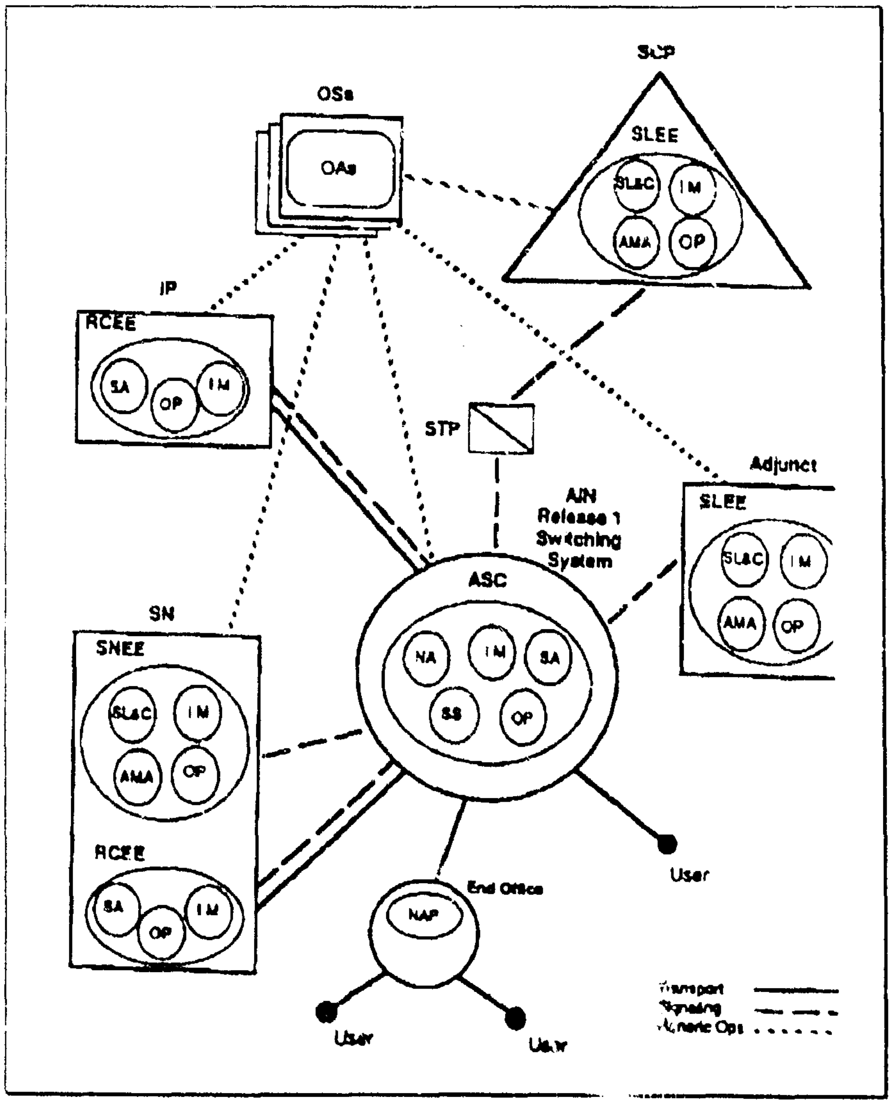
OA functions are divided into several domains that are responsible for various facets of operations tasks in the network. Such functions are implemented through an interaction between OA's and the operations capabilities in functional groups. The OA domains are:

- Service Negotiation and Management (SN&M)
- Service Provisioning (SP)
- Memory Administration (MA)
- Network Surveillance (NS)
- Network Services Testing (NT)
- Network Traffic Management (NTM)
- Network Data Collection (NDC)

- Repair Service Answering, and Work and Force Administration (RSA/WFA)
- Billing
- Planning and Engineering (P&E)

### A.2.2 Physical

The main components of the AIN physical architecture appear in the schematic diagram reproduced here as figure 6. A brief description of these sub-systems (i.e. NE's) appear below.




source: *Advanced Intelligent Network Release 1, Network and Operations Plan*, Bell Communications Research, Special Report SR-NPL-001623, Issue 1, June 1990.

**Figure 6. AIN physical architecture**

- AIN Switching Systems

An AIN Switching System is any switching system that contains ASC functionality. As all other AIN systems communicate with the Switching System it forms the *hub* of the AIN architecture.

- SCP's (Service Control Points) and Adjuncts

An SCP is where the AIN services actually reside. SCP's (or Adjuncts) cannot communicate with one another; nor can SCP's communicate with Adjuncts. A single AIN Switching System can connect to multiple SCP's (via Signal Transfer Points) and/or multiple Adjuncts. Similarly, multiple Adjuncts can connect to multiple AIN Switching Systems. A SCP node "serves as the communication channel between a SLEE and all external entities, providing basic message handling functions for all incoming and outgoing messages related to services, operations, and billing". An Adjunct is a "standalone network system" which has the same functionality as an SCP, but communicating directly and at a far higher speed (i.e. 45 Mb/s) with the AIN Switching System.

- SN's (Service Nodes)

SN's control AIN services, along with the resources needed to exchange information with users. A single AIN Switching System can be connected to multiple SN's, and *vice versa*. "SCP's, Adjuncts, and SN's can communicate with SN's only for the purpose of using resources residing in the SN's and with IP's".

- IP's (Intelligent Peripheral)

IP's offer the functionality and resources needed to exchange information with users, such as "voice announcements, voice recognition, and DTMF digit collection, and contains switching fabric to connect users to these resources". An IP (or multiples thereof) can only be connected to AIN Switching Systems (and not to one another).

- OS's (Operations Systems)

OS's are network systems that implement functions from one or more OA; furthermore, the functions of OA's may be implemented by more than one OS.

- Signal Transfer Points (STP's)

STP's are "treated as part of the Common Channel Signalling (CCS) network".

- Network Access Point (NAP)

NAP's allow non-AIN Switching Systems to access a limited set of AIN services. They detect triggers but cannot communicate with the SCP and therefore detected IN calls are routed to an SSP for handling [BUS91].

## A.3 Call Processing

- request for service

To begin with, Call Processing determines if a call request event at an AIN Switching System is in fact a request for an AIN service. This task proceeds as the ASC examines internal

information (i.e. trigger criteria) and (perhaps) information provided by the user (such as the dialled number).

- ASC to SLEE message passing

In response to a request for service, an ASC interacts with a SLEE in an SCP or Adjunct by passing a message which takes the form of a *logical representation of the call*. The SLEE acts on this message by selecting a corresponding SLP, which is executed only to produce further call processing instructions.

- SLEE to ASC message passing

Messages from a SLEE to an ASC serve two purposes. In one case, a SLEE passes messages "on behalf of the SLP" which subsequently cause the ASC to perform actions such as the routing of a call to a destination, or the sending of information to the user. The other case involves a request from an SLEE for an ASC to report on call events for a specific call.

## DISTRIBUTION

| | |
|---|---|
| Chief Defence Scientist and members of the DSTO Central Office Executive | 1 shared copy |
| Assistant Secretary Scientific Analysis | 1 copy |
| Counsellor, Defence Science, London | Doc Control Sheet |
| Counsellor, Defence Science, Washington | Doc Control Sheet |
| | |
| Senior Defence Scientific Adviser | 1 copy |
| Scientific Adviser - Polcom | 1 copy |
| Navy Scientific Adviser (NSA) | 1 copy |
| Scientific Adviser - Army (SA-A) | 1 copy |
| Air Force Scientific Adviser (AFSA) | 1 copy |
| | |
| Development Division | |
| Director General, Force Development (Joint) - DGFD (Joint) | 1 copy |
| Director General, Force Development (Land) - DGFD (Land) | 1 copy |
| Director General, Force Development (Air) - DGFD (Air) | 1 copy |
| Director General, Force Development (Sea) - DGFD (Sea) | 1 copy |
| Director Communications Development - DCD | 1 copy |
| Director Communications and Information System Policies and Plans - DCISPP | 1 copy |
| Operations Division | |
| Director General, Joint Communications and Electronics - DGJCE | 1 copy |
| Force Development and Analysis Division | |
| Assistant Secretary, Project Development - ASPD | 1 copy |
| Defence Materiel Division | |
| Director General, Joint Projects Management Branch - DGJPM | 1 copy |
| Assistant Secretary, Communications and Info. Systems Eng. Branch - ASCISE | 1 copy |
| Director, Communication Engineering Development - DCED | 1 copy |
| Science Policy Division | |
| Senior Defence Scientific Adviser - SDSA | 1 copy |
| Electronics Research Laboratory | |
| Director, Electronics Research Laboratory - DERL | 1 copy |
| Chief, Communications Division - CCD | 1 copy |
| Chief, Information Technology Division - CITD | 1 copy |
| Research Leader, Military Communications - RLMC | 1 copy |
| Research Leader, Secure Communications - RLSC | 1 copy |
| Research Leader, Military Computing Systems - RLMCS | 1 copy |
| Research Leader, Command and Control and Intelligence Systems - RLCCIS | 1 copy |
| Head, Switched Networks - HSN | 1 copy |
| Author, Wolf Getto | 1 copy |

| | |
|---|---|
| Joint Intelligence Organisation | |
| Deputy Director, Joint Intelligence Organisation - DDJIO | 1 copy |
| Defence Signals Directorate | |
| Director, Defence Signals Directorate | 1 copy |
| | |
| Defence Central Library - Technical Reports Centre | 1 copy |
| Manager Document Exchange Centre (MDEC) (for retention) | 1 copy |
| | |
| Additional copies which are to be sent through MDEC DIS for distribution: | |
| Defence Research Information Centre, United Kingdom | 2 copies |
| National Technical Information Service, United States | 2 copies |
| Director Scientific Information Services, Canada | 1 copy |
| Ministry of Defence New Zealand | 1 copy |
| National Library of Australia | 1 copy |
| | |
| Director of Publishing Laboratory | 1 copy |
| Defence Science and Technology Organisation Salisbury, Research Library | 2 copies |
| AGPS | 1 copy |
| Library, Defence Signals Directorate Canberra | 1 copy |
| British Library Document Supply Centre | 1 copy |
| | |
| SPARES | |
| Defence Science and Technology Organisation Salisbury, Research Library | 6 copies |

Department of Defence

**DOCUMENT CONTROL DATA SHEET**

| | |
|---|---|
| 1. Page Classification | UNCLASSIFIED |
| 2. Privacy Marking/Caveat ( of document ) | UNCLASSIFIED |

| | | | |
|---|---|---|---|
| 3a. AR Number<br>AR-008-866 | 3b. Laboratory Number<br>ERL-0825-RE | 3c. Type of Report<br>REPORT | 4. Task Number<br>ADF 92/515.1 |
| 5. Document Date<br>FEB 94 | 6. Cost Code<br>823886 | 7. Security Classification | 8. No. of Pages 32 |
| | | | 9. No. of Refs. 26 |

7. Security Classification

| Document | Title | Abstract |
|---|---|---|
| •U | U | U |

S (Secret) C (Confi ) R (Rest) U (Unclass)

* For UNCLASSIFIED docs with a secondary distribution LIMITATION, use (L) in document box.

10. Title

AN INTRODUCTION TO INTELLIGENT NETWORKS

11. Author(s)

Wolf Getto

12. Downgrading/Delimiting Instructions

N/A

13a. Corporate Author and Address

Electronics Research Laboratory
PO Box 1500, Salisbury SA 5108

13b. Task Sponsor

DORIC

14. Officer/Position responsible for

Security:.............N/A..........................................

Downgrading:........DERL.......... ..................................

Approval for Release:......DERL ................................ .

15 Secondary Release Statement of this Document

APPROVED FOR PUBLIC RELEASE

16a. Deliberate Announcement

No Limitation

16b. Casual Announcement (for citation in other documents)

[x] No Limitation [ ] Ref. by Author , Doc No. and date only.

17. DEFTEST Descriptors

INTELLIGENT NETWORKS
MILITARY COMMUNICATION

18. DISCAT Subject Codes

25

19. Abstract

Intelligent networking is a new and developing technology that is already having significant impact on telecommunications architectures. This paper offers a summary of this technology, concluding with a brief discussion of how it is likely to affect the military communications of the ADF.